Cited Ref. 6

(19)日本国特許庁（ＪＰ）　(12)**公開特許公報（Ａ）**　(11)特許出願公開番号
特開2001－283320
（P2001－283320A）
(43)公開日　平成13年10月12日(2001.10.12)

(51)Int.Cl.[7]	識別記号	ＦＩ		テーマコード（参考）
Ｇ０７Ｆ　17/00		Ｇ０７Ｆ　17/00	Ｂ	５Ｂ０４９
Ｇ０６Ｆ　17/60	３０２	Ｇ０６Ｆ　17/60	３０２Ｅ	５Ｃ０６４
	５１２		５１２	５Ｄ０４４
Ｇ１０Ｋ　15/02		Ｇ１０Ｋ　15/02		５Ｊ１０４
Ｇ１１Ｂ　20/10		Ｇ１１Ｂ　20/10	Ｈ	

審査請求　未請求　請求項の数８　ＯＬ　（全 15 頁）　最終頁に続く

(21)出願番号　特願2000－96883(P2000－96883)

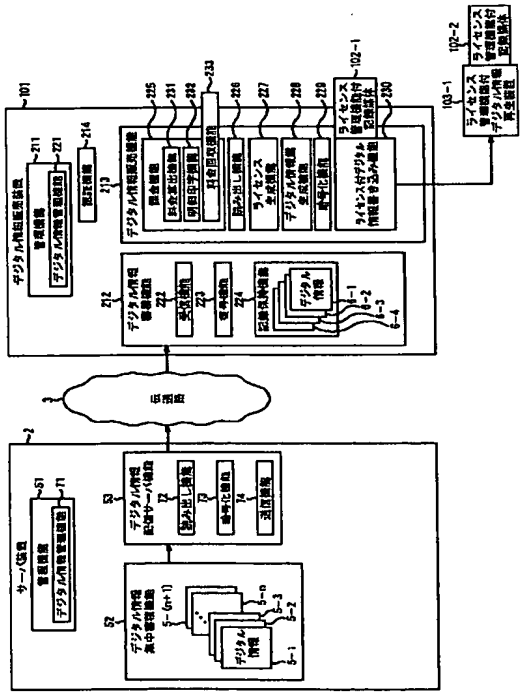
(22)出願日　平成12年３月31日(2000.3.31)

(71)出願人　000002185
ソニー株式会社
東京都品川区北品川６丁目７番35号
(72)発明者　岸　治彦
東京都品川区北品川６丁目７番35号　ソニー株式会社内
(72)発明者　栗原　章
東京都品川区北品川６丁目７番35号　ソニー株式会社内
(74)代理人　100082131
弁理士　稲本　義雄

最終頁に続く

(54)【発明の名称】　情報販売装置および方法、並びにプログラム格納媒体

(57)【要約】
【課題】　販売した情報の不正な利用を防止する。
【解決手段】　デジタル情報蓄積機能２１２は、販売するデジタル情報６を蓄積する。ライセンス生成機能２２７は、デジタル情報６に対応する利用条件を生成する。暗号化機能２２９は、デジタル情報６を暗号化する。デジタル情報鍵生成機能２２８は、暗号化されたデジタル情報６を復号する暗号鍵を生成する。認証機能２１４は、デジタル情報販売装置１０１に装着されているライセンス管理機能付記録媒体１０２－１を認証する。ライセンス付デジタル情報書き込み機能２３０は、認証されたライセンス管理機能付記録媒体１０２－１に、暗号化されたデジタル情報６を利用条件および暗号鍵と共に書き込む。



【特許請求の範囲】

【請求項１】　販売する情報を蓄積する蓄積手段と、
前記情報に対応する利用条件を生成する利用条件生成手段と、
前記情報を暗号化する暗号化手段と、
暗号化された前記情報を復号する暗号鍵を生成する暗号鍵生成手段と、
自分自身に装着されている記録媒体を認証する認証手段と、
前記認証手段により認証された前記記録媒体に、暗号化された前記情報を前記利用条件および前記暗号鍵と共に書き込む書き込み手段とを含むことを特徴とする情報販売装置。

【請求項２】　前記記録媒体に記録されている前記情報を再生する再生装置と通信する通信手段を更に含み、
前記認証手段は、前記通信手段が前記再生装置と通信するとき、前記再生装置を更に認証し、
前記書き込み手段は、前記再生装置を介して、前記記録媒体に、暗号化されている前記情報を前記利用条件および前記暗号鍵と共に書き込むことを特徴とする請求項１に記載の情報販売装置。

【請求項３】　前記通信手段は、前記再生装置に一体的に設けられている前記記録媒体に記録されている前記情報を再生する再生装置と通信し、
前記書き込み手段は、前記再生装置に一体的に設けられている前記記録媒体に、暗号化されている前記情報を前記利用条件および前記暗号鍵と共に書き込むことを特徴とする請求項２に記載の情報販売装置。

【請求項４】　所定の伝送路を介して送信された前記情報を受信する受信手段を更に含み、
前記蓄積手段は、前記受信手段が受信した前記情報を蓄積することを特徴とする請求項１に記載の情報販売装置。

【請求項５】　前記利用条件生成手段は、前記記録媒体に記録されている前記情報を再生する再生装置が従う前記利用条件を生成し、
前記暗号化手段は、前記再生装置が復号可能な方式で前記情報を暗号化することを特徴とする請求項１に記載の情報販売装置。

【請求項６】　前記情報は、プログラム、音声、音楽、静止画像、動画像、およびテキストの少なくとも１つを含むことを特徴とする請求項１に記載の情報販売装置。

【請求項７】　販売する情報を蓄積する蓄積ステップと、
前記情報に対応する利用条件を生成する利用条件生成ステップと、
前記情報を暗号化する暗号化ステップと、
暗号化された前記情報を復号する暗号鍵を生成する暗号鍵生成ステップと、
装着されている記録媒体を認証する認証ステップと、

前記認証ステップの処理で認証された前記記録媒体に、暗号化された前記情報を前記利用条件および前記暗号鍵と共に書き込む書き込みステップとを含むことを特徴とする情報販売方法。

【請求項８】　販売する情報を蓄積する蓄積ステップと、
前記情報に対応する利用条件を生成する利用条件生成ステップと、
前記情報を暗号化する暗号化ステップと、
暗号化された前記情報を復号する暗号鍵を生成する暗号鍵生成ステップと、
装着されている記録媒体を認証する認証ステップと、
前記認証ステップの処理で認証された前記記録媒体に、暗号化された前記情報を前記利用条件および前記暗号鍵と共に書き込む書き込みステップとを含むことを特徴とするコンピュータが読み取り可能なプログラムが格納されているプログラム格納媒体。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】本発明は、情報販売装置および方法、並びにプログラム格納媒体に関し、特に、音楽のデータなどの情報を販売する情報販売装置および方法、並びにプログラム格納媒体に関する。

【０００２】

【従来の技術】図１は、従来のデジタル情報販売システムの構成を説明する図である。デジタル情報販売装置１は、販売店（いわゆる、コンビニエンスストアなど）の店頭などに設置され、伝送路３を介して、サーバ装置２から送信されたデジタル情報を受信して、その内部に記録する。デジタル情報販売装置１は、その内部に記録しているデジタル情報を販売するとき、購入者が所有する記録媒体４が装着され、装着されている記録媒体４にデジタル情報を記録させる。

【０００３】デジタル情報販売装置１は、管理機能１１、デジタル情報蓄積機能１２、およびデジタル情報販売機能１３を有する。管理機能１１は、デジタル情報管理機能２１を有し、デジタル情報蓄積機能１２およびデジタル情報販売機能１３を制御する。

【０００４】デジタル情報蓄積機能１２は、受信機能２２、復号機能２３、および記録保持機能２４から構成される。受信機能２２は、伝送路３を介して、サーバ装置２から送信された暗号化されているデジタル情報を受信して、復号機能２３に供給する。

【０００５】復号機能２３は、予め、鍵を記憶し、復号機能２３から供給された、暗号化されているデジタル情報を復号する。記録保持機能２４は、復号機能２３から供給された、復号されたデジタル情報を、デジタル情報６－１乃至６－４として記録する。

【０００６】デジタル情報販売機能１３は、課金機能２５、読み出し機能２６、および書き込み機能２７から構

成される。

【０００７】課金機能２５は、デジタル情報蓄積機能１２に記録されているデジタル情報６－１乃至６－４を販売するとき、購入者から料金を徴収する。課金機能２５は、更に、料金算出機能３１、明細印字機能３２、および料金回収機能３３から構成される。

【０００８】料金算出機能３１は、販売するデジタル情報６－１乃至６－４の価格を算出する。明細印字機能３２は、デジタル情報６－１乃至６－４を販売するとき、領収書に販売価格などを印刷して出力する。

【０００９】料金回収機能３３は、購入者により挿入された代金に対応する貨幣から、販売するデジタル情報６－１乃至６－４の価格に対応する料金を回収する。

【００１０】読み出し機能２６は、販売するデジタル情報６－１乃至６－４の価格に対応する料金が支払われたとき、購入者の選択に基づいて、デジタル情報蓄積機能１２が蓄積しているデジタル情報６－１乃至６－４のいずれかを読み出して、読み出したデジタル情報６－１乃至６－４のいずれかを書き込み機能２７に供給する。

【００１１】書き込み機能２７は、読み出し機能２６から供給されたデジタル情報６－１乃至６－４のいずれかを、装着されている記録媒体４に書き込む。

【００１２】以下、デジタル情報６－１乃至６－４を個々に区別する必要がないとき、単に、デジタル情報６と称する。

【００１３】サーバ装置２は、予め定めた時刻（例えば、毎日の午前０時）に、予め記録しているデジタル情報５－１乃至５－（ｎ＋１）の中からデジタル情報販売装置１に送信するものを選択して、選択したデジタル情報５－１乃至５－（ｎ＋１）のいずれかを、伝送路３を介して、デジタル情報販売装置１に送信する。

【００１４】サーバ装置２は、管理機能５１、デジタル情報集中蓄積機能５２、およびデジタル情報配信サーバ機能５３を有する。管理機能５１は、デジタル情報管理機能７１を有し、デジタル情報集中蓄積機能５２およびデジタル情報配信サーバ機能５３を制御する。

【００１５】デジタル情報集中蓄積機能５２は、デジタル情報販売装置１に送信するためのデジタル情報５－１乃至５－（ｎ＋１）を蓄積する。

【００１６】デジタル情報配信サーバ機能５３は、デジタル情報集中蓄積機能５２から蓄積されているデジタル情報５－１乃至５－（ｎ＋１）を読み出して、暗号化して、伝送路３を介して、デジタル情報販売装置１に送信する。デジタル情報配信サーバ機能５３は、読み出し機能７２、暗号化機能７３、および送信機能７４を有する。

【００１７】読み出し機能７２は、デジタル情報集中蓄積機能５２から蓄積されているデジタル情報５－１乃至５－（ｎ＋１）のいずれかを読み出して、暗号化機能７３に供給する。暗号化機能７３は、読み出し機能７２から供給されたデジタル情報５－１乃至５－（ｎ＋１）のいずれかを、DES（Data Encryption Standard）などの方式で暗号化して、送信機能７４に供給する。送信機能７４は、暗号化されたデジタル情報５－１乃至５－（ｎ＋１）のいずれかを、伝送路３を介して、デジタル情報販売装置１に送信する。

【００１８】以下、デジタル情報５－１乃至５－（ｎ＋１）を個々に区別する必要がないとき、単にデジタル情報５と称する。

【００１９】

【発明が解決しようとする課題】しかしながら、記録媒体４には、不正なコピーまたは再生など、本来許可されていない利用を防止する機能が無く、また、デジタル情報６に対応する利用条件等も記録媒体４に記録されないので、販売されたデジタル情報について、不正な利用を防止することができないという問題点があった。

【００２０】本発明はこのような状況に鑑みてなされたものであり、販売した情報の不正な利用の防止ができるようにすることを目的とする。

【００２１】

【課題を解決するための手段】請求項１に記載の情報販売装置は、販売する情報を蓄積する蓄積手段と、情報に対応する利用条件を生成する利用条件生成手段と、情報を暗号化する暗号化手段と、暗号化された情報を復号する暗号鍵を生成する暗号鍵生成手段と、自分自身に装着されている記録媒体を認証する認証手段と、認証手段により認証された記録媒体に、暗号化された情報を利用条件および暗号鍵と共に書き込む書き込み手段とを含むことを特徴とする。

【００２２】情報販売装置は、記録媒体に記録されている情報を再生する再生装置と通信する通信手段を更に設け、認証手段が、通信手段が再生装置と通信するとき、再生装置を更に認証し、書き込み手段が、再生装置を介して、記録媒体に、暗号化されている情報を利用条件および暗号鍵と共に書き込むようにすることができる。

【００２３】通信手段は、再生装置に一体的に設けられている記録媒体に記録されている情報を再生する再生装置と通信し、書き込み手段は、再生装置に一体的に設けられている記録媒体に、暗号化されている情報を利用条件および暗号鍵と共に書き込むようにすることができる。

【００２４】情報販売装置は、所定の伝送路を介して送信された情報を受信する受信手段を更に設け、蓄積手段が、受信手段が受信した情報を蓄積するようにすることができる。

【００２５】利用条件生成手段は、記録媒体に記録されている情報を再生する再生装置が従う利用条件を生成し、暗号化手段は、再生装置が復号可能な方式で情報を暗号化するようにすることができる。

【００２６】情報は、プログラム、音声、音楽、静止画

像、動画像、およびテキストの少なくとも１つを含むようにすることができる。

【００２７】請求項７に記載の情報販売方法は、販売する情報を蓄積する蓄積ステップと、情報に対応する利用条件を生成する利用条件生成ステップと、情報を暗号化する暗号化ステップと、暗号化された情報を復号する暗号鍵を生成する暗号鍵生成ステップと、装着されている記録媒体を認証する認証ステップと、認証ステップの処理で認証された記録媒体に、暗号化された情報を利用条件および暗号鍵と共に書き込む書き込みステップとを含むことを特徴とする。

【００２８】請求項８に記載のプログラム格納媒体のプログラムは、販売する情報を蓄積する蓄積ステップと、情報に対応する利用条件を生成する利用条件生成ステップと、情報を暗号化する暗号化ステップと、暗号化された情報を復号する暗号鍵を生成する暗号鍵生成ステップと、装着されている記録媒体を認証する認証ステップと、認証ステップの処理で認証された記録媒体に、暗号化された情報を利用条件および暗号鍵と共に書き込む書き込みステップとを含むことを特徴とする。

【００２９】請求項１に記載の情報販売装置、請求項７に記載の情報販売方法、および請求項８に記載のプログラム格納媒体においては、販売する情報が蓄積され、情報に対応する利用条件が生成され、情報が暗号化され、暗号化された情報を復号する暗号鍵が生成され、装着されている記録媒体が認証され、認証された記録媒体に、暗号化された情報が利用条件および暗号鍵と共に書き込まれる。

【００３０】

【発明の実施の形態】図２は、本発明に係るデジタル情報販売システムの一実施の形態を説明する図である。デジタル情報販売装置１０１は、販売店（いわゆる、コンビニエンスストアなど）の店頭などに設置され、伝送路３を介して、サーバ装置２から送信されたデジタル情報（プログラム、またはテキスト、楽音を含む音楽、音声、若しくは静止画像、動画像のデータなど）を受信して、その内部に記録する。

【００３１】デジタル情報販売装置１０１は、例えば、音楽データであるデジタル情報を販売する場合、ＳＤＭＩ（Secure Digital Music Initiative）の規格に準拠して、デジタル情報に対応する利用条件を生成すると共に暗号鍵（以下、デジタル情報鍵と称する）を生成して、デジタル情報をデジタル情報鍵で復号できるように暗号化して、デジタル情報を利用条件およびデジタル情報鍵と共に、ライセンス管理機能付記録媒体１０２－１またはライセンス管理機能付デジタル情報再生装置１０３－１に供給する。

【００３２】デジタル情報販売装置１０１は、DESなどの共通鍵暗号方式で、デジタル情報を暗号化するとき、デジタル情報鍵でデジタル情報を暗号化する。デジタル情報販売装置１０１は、RSA（Rivest-Shamir-Adleman）などの公開鍵暗号方式で、デジタル情報を暗号化するとき、秘密鍵でデジタル情報を暗号化して、公開鍵をデジタル情報鍵として、ライセンス管理機能付記録媒体１０２－１またはライセンス管理機能付デジタル情報再生装置１０３－１に供給する。

【００３３】例えば、音楽データであるデジタル情報を利用する場合、ライセンス管理機能付デジタル情報再生装置１０３－１および１０３－２、パーソナルコンピュータ１０４、並びに携帯端末装置１０５は、ＳＤＭＩの規格に準拠したソフトウェアモジュールであるＬＣＭ（Licensed Compliant Module）を有し、デジタル情報に対応する利用条件に基づいて、デジタル情報の、例えば、いわゆる、チェックイン、チェックアウト、コピー、または移動などを許可するか、または禁止する。

【００３４】ライセンス管理機能付記録媒体１０２－１および１０２－２は、デジタル情報に対応する利用条件に基づいて、記録しているデジタル情報の利用を管理する（例えば、読み出しを許可または禁止する）。

【００３５】伝送路３は、有線または無線の通信路であり、例えば、専用線、LAN（Local Area Network）、ISDN（Integrated Services Digital Network）、xDSL（x Digital Subscriber Line）、電話回線、PHS（Personal Handyphone System）回線、携帯電話回線、WLL（Wireless Local Loop）回線、通信衛星回線、または放送衛星回線などである。

【００３６】デジタル情報販売装置１０１は、その内部に記録しているデジタル情報６を購入するために、購入者が所有するライセンス管理機能付記録媒体１０２－１が装置着部１１１に装着されたとき、ライセンス管理機能付記録媒体１０２－１との相互認証の処理を実行する。デジタル情報販売装置１０１は、デジタル情報６に対応する利用条件を生成するとともに、デジタル情報６を暗号化して、デジタル情報６を復号するデジタル情報鍵を生成する。

【００３７】デジタル情報販売装置１０１は、認証されたライセンス管理機能付記録媒体１０２－１に暗号化されているデジタル情報６を、利用条件およびデジタル情報鍵と共に記録させる。

【００３８】デジタル情報販売装置１０１によりデジタル情報６が記録されたライセンス管理機能付記録媒体１０２－１は、例えば、ライセンス管理機能付デジタル情報再生機能１１４を有する、例えば、PDA（Personal Digital Assistant）、または携帯電話機などの携帯端末装置１０５に装着される。携帯端末装置１０５のライセンス管理機能付デジタル情報再生機能１１４は、ライセンス管理機能付記録媒体１０２－１に記録されたデジタル情報６を読み出して、そのデジタル情報６に対応する利用条件に基づき、読み出したデジタル情報６を利用することができる。

【００３９】購入者が所有するライセンス管理機能付記録媒体１０２－２が装着されているライセンス管理機能付デジタル情報再生装置１０３－１のインターフェース１１３－１は、例えば、インターフェース１１３－１およびインターフェース１１２の通信方式に対応するケーブル等を介して、デジタル情報販売装置１０１のインターフェース１１２と接続される。デジタル情報販売装置１０１は、ライセンス管理機能付デジタル情報再生装置１０３－１が接続されたとき、ライセンス管理機能付デジタル情報再生装置１０３－１との相互認証の処理を実行する。

【００４０】なお、ライセンス管理機能付デジタル情報再生装置１０３－１は、ライセンス管理機能付記録媒体１０２－２が装着されたとき、ライセンス管理機能付記録媒体１０２－２との相互認証の処理を実行する。

【００４１】デジタル情報販売装置１０１は、認証されたライセンス管理機能付デジタル情報再生装置１０３－１に装着されているライセンス管理機能付記録媒体１０２－２に、ライセンス管理機能付デジタル情報再生装置１０３－１を介して、デジタル情報６を利用条件およびデジタル情報鍵と共に記録させる。

【００４２】また、ライセンス管理機能付デジタル情報再生装置１０３－１は、その内部に一体的に設けられた記憶部に、デジタル情報販売装置１０１から供給されたデジタル情報６を、利用条件およびデジタル情報鍵と共に記憶させるようにしてもよい。

【００４３】デジタル情報販売装置１０１によりデジタル情報６が記録されたライセンス管理機能付記録媒体１０２－２は、例えば、インターフェース１１３－２およびインターフェース１１４を介して、パーソナルコンピュータ１０４に接続されているライセンス管理機能付デジタル情報再生装置１０３－２に装着される。ライセンス管理機能付デジタル情報再生装置１０３－２は、そのデジタル情報６に対応する利用条件に基づき、ライセンス管理機能付記録媒体１０２－２に記録されたデジタル情報６を読み出して、読み出したデジタル情報６を利用することができる。

【００４４】ライセンス管理機能付記録媒体１０２－１または１０２－２は、例えば、フラッシュメモリなどの半導体メモリ、フロッピー（登録商標）ディスクなどの磁気ディスク、コンパクトディスク（商標）などの光ディスク、またはミニディスク（商標）などの光磁気ディスクなどで構成される。

【００４５】また、パーソナルコンピュータ１０４は、そのデジタル情報６に対応する利用条件に基づき、ライセンス管理機能付デジタル情報再生装置１０３－２を介して、ライセンス管理機能付記録媒体１０２－２に記録されたデジタル情報６を読み出して、読み出したデジタル情報６を利用することができる。

【００４６】なお、インターフェース１１２、インターフェース１１３－１および１１３－２、並びにインターフェース１１４は、USB（Universal Sirial Bus）、IEEE（Institute of Electrical and Electronics Engineers）1394、若しくはSCSI（Small Computer System Interface）などの有線の通信方式、またはIrDA（Infrared Data Association）が定める赤外線通信、若しくはBluetoothなどの無線の通信方式を利用することができる。

【００４７】図３は、デジタル情報販売装置１０１の構成の例を説明する図である。ＣＰＵ（Central Processing Unit）１２１は、各種アプリケーションプログラムや、ＯＳ（Operating System）などを実際に実行する。ＲＯＭ（Read-only Memory）１２２は、一般的には、ＣＰＵ１２１が使用するプログラムや演算用のパラメータのうちの基本的に固定のデータを格納する。ＲＡＭ（Random-Access Memory）１２３は、ＣＰＵ１２１の実行において使用するプログラムや、その実行において適宜変化するパラメータを格納する。

【００４８】入力部１２５は、表示部１２６上に設けられたタッチパッド、または入力キーなどから構成され、ＣＰＵ１２１に各種の指令を入力するとき、購入者により操作される。表示部１２６は、液晶表示装置またはＣＲＴ（Cathode Ray Tube）などから成り、各種情報をテキストやイメージで表示する。音声再生部１２７は、例えば、ＣＰＵ１２１から供給されたデジタル情報６に含まれる音楽のデータなどを基に、音声を出力する。

【００４９】通信部１２８は、伝送路３を介して、サーバ装置２から送信されたパケットに格納されているデジタル情報などのデータをＣＰＵ１２１、ＲＡＭ１２３、または記録部１２９に出力する。

【００５０】記録部１２９は、ＨＤＤ（Hard Disk Drive）などで構成され、それらにＣＰＵ１２１によって実行するプログラムやデジタル情報６を記録または再生させる。

【００５１】ドライブ５３は、装着されている磁気ディスク６１、光ディスク６２、光磁気ディスク６３、または半導体メモリ６４に記録されているデータまたはプログラムを読み出して、そのデータまたはプログラムを、インターフェース１３０、およびバス１２４を介して接続されているＲＡＭ１２３に供給する。

【００５２】書き込み部１３１は、装着部１１１に装着されているライセンス管理機能付記録媒体１０２－１に、記録部１２９に記録されているデジタル情報６を書き込む。

【００５３】インターフェース１１２は、所定の通信方式に対応するケーブルの一端が接続され、そのケーブルの他の一端に接続されているライセンス管理機能付デジタル情報再生装置１０３－１に、記録部１２９に記録されているデジタル情報６を送信する。

【００５４】料金回収部１３２は、購入者により貨幣が投入され、貨幣が投入されたか否かを示す信号、および

投入された貨幣の額に対応する信号をＣＰＵ１２１に供給する。

【００５５】これらのＣＰＵ１２１乃至料金回収部１３２は、バス１２４により相互に接続されている。

【００５６】図４は、本発明に係るデジタル情報販売システムの一実施の形態の構成を説明する図である。図１に示す場合と同様の部分には、同一の番号を付してあり、その説明は省略する。

【００５７】デジタル情報販売装置１０１は、例えば、ＣＰＵ１２１の所定のプログラムの実行により実現される、管理機能２１１、デジタル情報蓄積機能２１２、デジタル情報販売機能２１３、および認証機能２１４を有する。管理機能２１１は、デジタル情報管理機能２２１を有し、例えば、購入者の操作に対応した入力部１２５の信号を基に、デジタル情報蓄積機能２１２およびデジタル情報販売機能２１３を制御する。

【００５８】デジタル情報蓄積機能２１２は、受信機能２２２、復号機能２２３、および記録保持機能２２４から構成される。受信機能２２２は、伝送路３を介して、サーバ装置２から送信された、暗号化されているデジタル情報５を受信して、復号機能２２３に供給する。

【００５９】復号機能２２３は、予め鍵を記憶し、復号機能２２３から供給された、暗号化されているデジタル情報５を復号する。記録保持機能２２４は、復号機能２２３から復号されたデジタル情報５を受信して、例えば、デジタル情報６－１乃至６－４として記録する。

【００６０】デジタル情報販売機能２１３は、課金機能２２５、読み出し機能２２６、ライセンス生成機能２２７、デジタル情報鍵生成機能２２８、暗号化機能２２９、およびライセンス付デジタル情報書き込み機能２３０から構成される。

【００６１】課金機能２２５は、デジタル情報蓄積機能２１２が蓄積しているデジタル情報６－１乃至６－４を販売するとき、購入者から販売するデジタル情報６－１乃至６－４の価格に対応する料金を徴収する。課金機能２２５は、更に、料金算出機能２３１、明細印字機能２３２、および料金回収機能２３３から構成される。

【００６２】料金算出機能２３１は、販売するデジタル情報６－１乃至６－４の価格を算出する。明細印字機能２３２は、デジタル情報６－１乃至６－４を販売するとき、領収書などに販売価格または販売価格に対応するバーコードなどを印刷して出力する。

【００６３】料金回収機能２３３は、料金回収部１３２の信号を基に、販売するデジタル情報６－１乃至６－４の価格に対応する料金を料金回収部１３２に回収させる。

【００６４】読み出し機能２２６は、販売するデジタル情報６－１乃至６－４の価格に対応する料金が支払われたとき、購入者の選択に対応する、デジタル情報蓄積機能２１２が蓄積しているデジタル情報６－１乃至６－４のいずれかを読み出して、読み出したデジタル情報６－１乃至６－４を暗号化機能２３０に供給する。

【００６５】ライセンス生成機能２２７は、購入者の操作に対応した入力部１２５からの信号などに基づいて、販売するデジタル情報６－１乃至６－４のそれぞれに対応する利用条件を生成して、ライセンス付デジタル情報書き込み機能２３０に供給する。

【００６６】デジタル情報鍵生成機能２２８は、販売するデジタル情報６－１乃至６－４のそれぞれに対応するデジタル情報鍵を生成して、暗号化機能２２９に供給する。

【００６７】暗号化機能２２９は、デジタル情報鍵生成機能２２８から供給されたデジタル情報鍵で復号できるように、読み出し機能２２６から供給されたデジタル情報６－１乃至６－４のそれぞれを暗号化する。暗号化機能２２９は、対応する利用条件と共に、デジタル情報６－１乃至６－４のそれぞれを暗号化するようにしてもよい。暗号化機能２２９は、暗号化したデジタル情報６－１乃至６－４を、デジタル情報鍵と共にライセンス付デジタル情報書き込み機能２３０に供給する。

【００６８】ライセンス付デジタル情報書き込み機能２３０は、暗号化機能２２９から供給されたデジタル情報６－１乃至６－４を、デジタル情報鍵および利用条件と共に、認証されたライセンス管理機能付記録媒体１０２－１に書き込む。また、ライセンス付デジタル情報書き込み機能２３０は、ライセンス管理機能付記録媒体１０２－２が装着されているライセンス管理機能付デジタル情報再生装置１０３－１に、暗号化されたデジタル情報６－１乃至６－４を、デジタル情報鍵および利用条件と共に書き込む。

【００６９】ライセンス管理機能付記録媒体１０２－１またはライセンス管理機能付デジタル情報再生装置１０３－１に供給されるデジタル情報６は、図５に示すように、デジタル情報６に対応する利用条件およびデジタル情報６を復号するためのデジタル情報鍵と対応付けられている。ライセンス管理機能付記録媒体１０２－１またはライセンス管理機能付デジタル情報再生装置１０３－１は、デジタル情報６を利用するとき、デジタル情報鍵でデジタル情報６を復号して、対応する利用条件に基づき、デジタル情報６を利用する。

【００７０】例えば、利用条件において、対応するデジタル情報６の移動は許可されているが、コピーは許可されていないとき、ライセンス管理機能付記録媒体１０２－１またはライセンス管理機能付デジタル情報再生装置１０３－１は、そのデジタル情報６を移動させるが、そのデジタル情報６を他の機器にコピーさせない。

【００７１】認証機能２１４は、後述する処理により、装着されたライセンス管理機能付記録媒体１０２－１、またはライセンス管理機能付記録媒体１０２－２が装着されているライセンス管理機能付デジタル情報再生装置

１０３－２（接続されている）を認証する。

【００７２】なお、管理機能２１１、デジタル情報蓄積機能２１２、デジタル情報販売機能２１３、および認証機能２１４は、それぞれ、専用のハードウェアで構成するようにしてもよい。

【００７３】次に、購入者の所有するライセンス管理機能付記録媒体１０２－１にデジタル情報６を書き込んでデジタル情報６を販売するときの、デジタル情報販売装置１０１のデジタル情報６の販売の処理を、図６のフローチャートを参照して説明する。ステップＳ１１において、管理機能２１１は、書き込み部１３１から供給される信号を基に、ライセンス管理機能付記録媒体１０２－１がデジタル情報販売装置１０１の装着部１１１に装着されたか否かを判定し、ライセンス管理機能付記録媒体１０２－１が装着部１１１に装着されていないと判定された場合、ライセンス管理機能付記録媒体１０２－１が装着されるまで、ステップＳ１１の判定の処理を繰り返す。

【００７４】ステップＳ１１において、ライセンス管理機能付記録媒体１０２－１が装着部１１１に装着されたと判定された場合、ステップＳ１２に進み、認証機能２１４は、装着部１１１に装着されているライセンス管理機能付記録媒体１０２－１との認証の処理を実行する。

【００７５】図７は、デジタル情報販売装置１０１の認証機能２１４とライセンス管理機能付記録媒体１０２－１との認証の処理を説明する図である。デジタル情報販売装置１０１の認証機能２１４とライセンス管理機能付記録媒体１０２－１との認証の処理は、例えば、チャレンジレスポンス方式で行われる。

【００７６】デジタル情報販売装置１０１は、予め、鍵Ｋａｂおよび自分自身のＩＤを記録している。ライセンス管理機能付記録媒体１０２－１は、予め、鍵K^*（複数の鍵から構成される）を記録している。

【００７７】デジタル情報販売装置１０１の認証機能２１４は、内部の乱数生成部で、乱数Ｎａおよび乱数＃Ｇを生成して、ＩＤと共に、乱数Ｎａおよび乱数＃Ｇをライセンス管理機能付記録媒体１０２－１に送信する。

【００７８】ライセンス管理機能付記録媒体１０２－１は、内部の乱数生成部で、乱数Ｎｂおよび乱数Ｓｂを生成する。ライセンス管理機能付記録媒体１０２－１は、デジタル情報販売装置１０１から送信された、デジタル情報販売装置１０１のＩＤ、乱数Ｎａ、および乱数＃Ｇを受信する。ライセンス管理機能付記録媒体１０２－１の算出部は、乱数＃Ｇに所定の関数を適用して、変数ｊを生成する。

【００７９】ライセンス管理機能付記録媒体１０２－１の算出部は、変数ｊを基に、複数の鍵から構成される鍵K^*の中から所定の鍵$K^*_{(j)}$を選択して、選択した鍵$K^*_{(j)}$を鍵として、デジタル情報販売装置１０１のＩＤにハッシュ関数を適用して、鍵Ｋａｂを求める。

【００８０】ライセンス管理機能付記録媒体１０２－１の算出部は、鍵Ｋａｂを鍵として、デジタル情報販売装置１０１から受信した乱数Ｎａ、生成した乱数Ｎｂ、およびデジタル情報販売装置１０１のＩＤにハッシュ関数を適用して、変数Ｒを算出する。

【００８１】ライセンス管理機能付記録媒体１０２－１は、乱数Ｎｂ、変数Ｒ、変数ｊ、および乱数Ｓｂをデジタル情報販売装置１０１に送信する。

【００８２】デジタル情報販売装置１０１は、ライセンス管理機能付記録媒体１０２－１が送信した、乱数Ｎｂ、変数Ｒ、変数ｊ、および乱数Ｓｂを受信する。

【００８３】デジタル情報販売装置１０１の認証機能２１４は、鍵Ｋａｂを鍵として、乱数Ｎａ、ライセンス管理機能付記録媒体１０２－１から受信した乱数Ｎｂ、および自分自身のＩＤにハッシュ関数を適用して算出された値が、ライセンス管理機能付記録媒体１０２－１から受信した変数Ｒと等しいか否かを判定し、鍵Ｋａｂを鍵として、乱数Ｎａ、乱数Ｎｂ、およびＩＤにハッシュ関数を適用して算出された値が変数Ｒと等しいと判定された場合、ライセンス管理機能付記録媒体１０２－１を正当であると認証する。

【００８４】鍵Ｋａｂを鍵として、乱数Ｎａ、乱数Ｎｂ、およびＩＤにハッシュ関数を適用して算出された値が変数Ｒと等くないと判定された場合、デジタル情報販売装置１０１の認証機能２１４は、ライセンス管理機能付記録媒体１０２－１が正当でないと判定し、ライセンス管理機能付記録媒体１０２－１を認証せず、処理は終了する。

【００８５】ライセンス管理機能付記録媒体１０２－１を正当であると認証された場合、デジタル情報販売装置１０１の認証機能２１４は、鍵Ｋａｂを鍵として、乱数Ｎｂおよび乱数Ｎａにハッシュ関数を適用して、変数Ｒ’を算出する。デジタル情報販売装置１０１の認証機能２１４は、鍵Ｋａｂを鍵として、乱数Ｓａおよび乱数Ｓｂにハッシュ関数を適用して、一時鍵Ｋｓを算出する。

【００８６】デジタル情報販売装置１０１の認証機能２１４は、変数Ｒ’および乱数Ｓａをライセンス管理機能付記録媒体１０２－１に送信する。

【００８７】ライセンス管理機能付記録媒体１０２－１は、デジタル情報販売装置１０１から送信された変数Ｒ’および乱数Ｓａを受信する。

【００８８】ライセンス管理機能付記録媒体１０２－１は、鍵Ｋａｂを鍵として、乱数Ｎｂ、および乱数Ｎａにハッシュ関数を適用して算出された値が、ライセンス管理機能付記録媒体１０２－１から受信した変数Ｒ’と等しいか否かを判定し、鍵Ｋａｂを鍵として、乱数Ｎｂ、および乱数Ｎａにハッシュ関数を適用して算出された値が、変数Ｒ’と等しいと判定された場合、デジタル情報販売装置１０１を正当であると認証する。

【００８９】鍵Ｋａｂを鍵として、乱数Ｎｂ、および乱数Ｎａにハッシュ関数を適用して算出された値が、変数Ｒ’と等くないと判定された場合、ライセンス管理機能付記録媒体１０２－１は、デジタル情報販売装置１０１が正当でないと判定し、デジタル情報販売装置１０１を認証せず、処理は終了する。

【００９０】デジタル情報販売装置１０１が正当であると認証された場合、ライセンス管理機能付記録媒体１０２－１は、鍵Ｋａｂを鍵として、乱数Ｓａおよび乱数Ｓｂにハッシュ関数を適用して、一時鍵Ｋｓを算出する。

【００９１】このように、デジタル情報販売装置１０１とライセンス管理機能付記録媒体１０２－１とは、相互認証すると共に、相互認証されたとき、共通の一時鍵Ｋｓを共有する。

【００９２】なお、認証の処理で利用されるハッシュ関数として、DESを利用するようにしてもよい。

【００９３】ステップＳ１３において、管理機能２１１は、ステップＳ１２の処理でライセンス管理機能付記録媒体１０２－１が認証されたか否かを判定し、ライセンス管理機能付記録媒体１０２－１が認証されたと判定された場合、ステップＳ１４に進み、デジタル情報蓄積機能２１２から供給されるデータを基に、表示部１２６に、販売可能なデジタル情報６の選択画面を表示させる。

【００９４】ステップＳ１５において、管理機能２１１は、購入者の操作に対応した入力部１２５からの信号を基に、販売するデジタル情報６が決定されたか否かを判定し、販売するデジタル情報６が決定されたと判定された場合、ステップＳ１６に進み、デジタル情報販売機能２１３の料金算出機能２３１に、販売するデジタル情報６の価格を算出させる。

【００９５】ステップＳ１７において、管理機能２１１は、デジタル情報販売機能２１３の料金回収部１３２からの信号を基に、料金回収部１３２に代金が投入されたか否かを判定し、料金回収部１３２に代金が投入されたと判定された場合、ステップＳ１８に進み、料金回収部１３２に投入された代金を料金回収機能２３３に数えさせる。

【００９６】ステップＳ１９において、管理機能２１１は、ステップＳ１６で算出されたデジタル情報６の価格、および料金回収機能２３３から供給された、料金回収部１３２に投入された代金に対応する信号を基に、投入された代金でデジタル情報６が販売できるか否かを判定し、投入された代金でデジタル情報６が販売できると判定された場合、ステップＳ２０に進み、読み出し機能２２６に、記録保持機能２２４から所定のデジタル情報６を読み出させる。ライセンス生成機能２２７は、読み出したデジタル情報６に対応する利用条件を生成する。デジタル情報鍵生成機能２２８は、デジタル情報６を復号するデジタル情報鍵を生成する。暗号化機能２２９は、例えば、DESの方式で、デジタル情報６を暗号化する。

【００９７】ライセンス付デジタル情報書き込み機能２３０は、デジタル情報鍵および利用条件と共に、ライセンス管理機能付記録媒体１０２－１にデジタル情報６を記録する。

【００９８】ステップＳ２１において、管理機能２１１は、書き込み部１３１、またはライセンス付デジタル情報書き込み機能２３０から供給される信号を基に、デジタル情報鍵および利用条件と共に、ライセンス管理機能付記録媒体１０２－１にデジタル情報６が正常に記録されたか否かを判定し、デジタル情報鍵および利用条件と共に、ライセンス管理機能付記録媒体１０２－１にデジタル情報６が正常に記録されたと判定された場合、ステップＳ２２に進み、デジタル情報販売装置１０１の装着部１１１からライセンス管理機能付記録媒体１０２－１を排出させ、処理は終了する。

【００９９】ステップＳ１３において、ライセンス管理機能付記録媒体１０２－１が認証されないと判定された場合、ライセンス管理機能付記録媒体１０２－１が正当ではないので、ステップＳ２３に進み、管理機能２１１は、表示部１２６に認証されなかった旨を示すエラーメッセージを表示させ、処理は終了する。

【０１００】ステップＳ１５において、販売するデジタル情報６が決定されず、処理の中止が要求されたと判定された場合、ステップＳ２４に進み、管理機能２１１は、表示部１２６に処理が中断された旨を示すメッセージを表示させ、処理は終了する。

【０１０１】ステップＳ１７において、料金回収部１３２に代金が投入されず、処理の中止が要求されたと判定された場合、ステップＳ２５に進み、管理機能２１１は、表示部１２６に処理が中断された旨を示すメッセージを表示させ、処理は終了する。

【０１０２】ステップＳ１９において、投入された代金でデジタル情報６が販売できないと判定された場合、ステップＳ２６に進み、管理機能２１１は、表示部１２６に、代金が足りないので処理が中断された旨を示すメッセージを表示させ、料金回収部１３２に投入された代金を排出させて、処理は終了する。

【０１０３】ステップＳ２１において、デジタル情報鍵および利用条件と共に、ライセンス管理機能付記録媒体１０２－１にデジタル情報６が正常に記録されないと判定された場合、ステップＳ２７に進み、管理機能２１１は、表示部１２６に、書き込みが失敗した旨を示すエラーメッセージを表示させ、処理は終了する。

【０１０４】以上のように、デジタル情報販売装置１０１は、ライセンス管理機能付記録媒体１０２－１に、デジタル情報鍵および利用条件と共に、デジタル情報６を記録させることができる。

【０１０５】なお、デジタル情報販売装置１０１は、同

様の処理で、ライセンス管理機能付記録媒体１０２－２が装着されているライセンス管理機能付デジタル情報再生装置１０３－１に、デジタル情報鍵および利用条件と共にデジタル情報６を書き込む。

【０１０６】次に、購入者の所有するライセンス管理機能付記録媒体１０２－１にデジタル情報６を書き込んでデジタル情報６を販売するときの、デジタル情報販売装置１０１のデジタル情報６の販売の他の処理を、図８のフローチャートを参照して説明する。ステップＳ５１乃至ステップＳ５５の処理は、図６のステップＳ１１乃至ステップＳ１５の処理と、それぞれ同様であるので、その説明は省略する。

【０１０７】ステップＳ５５において、販売するデジタル情報６が決定されたと判定された場合、ステップＳ５６に進み、管理機能１１は、読み出し機能２２６に、記録保持機能２２４から販売が決定されたデジタル情報６を読み出させる。ライセンス生成機能２２７は、読み出したデジタル情報６に対応する利用条件を生成する。デジタル情報鍵生成機能２２８は、デジタル情報６を復号するデジタル情報鍵を生成する。暗号化機能２２９は、例えば、DESの方式で、デジタル情報６を暗号化する。

【０１０８】ライセンス付デジタル情報書き込み機能２３０は、デジタル情報鍵および利用条件と共に、ライセンス管理機能付記録媒体１０２－１にデジタル情報６を記録する。

【０１０９】ステップＳ５７において、管理機能２１１は、書き込み部１３１、またはライセンス付デジタル情報書き込み機能２３０から供給される信号を基に、デジタル情報鍵および利用条件と共に、ライセンス管理機能付記録媒体１０２－１にデジタル情報６が正常に記録されたか否かを判定し、デジタル情報鍵および利用条件と共に、ライセンス管理機能付記録媒体１０２－１にデジタル情報６が正常に記録されたと判定された場合、ステップＳ５８に進み、管理機能２１１は、デジタル情報販売機能２１３の料金算出機能２３１に、販売するデジタル情報６の価格を算出させる。

【０１１０】ステップＳ５９において、管理機能２１１は、明細印字機能２３２に、ステップＳ５８の処理で算出した販売するデジタル情報６の価格を、数字およびバーコードなどで領収書に印刷させる。

【０１１１】ステップＳ６０において、管理機能２１１は、デジタル情報販売装置１０１の装着部１１１からライセンス管理機能付記録媒体１０２－１を排出させる。

【０１１２】ステップＳ６１において、管理機能２１１は、料金回収機能２３３に、販売するデジタル情報６の価格に対応する、支払われた料金を受け取らせ、処理は終了する。

【０１１３】ステップＳ５３において、ライセンス管理機能付記録媒体１０２－１が認証されないと判定された場合、ライセンス管理機能付記録媒体１０２－１が正当ではないので、ステップＳ６２に進み、管理機能２１１は、表示部１２６に認証されなかった旨を示すエラーメッセージを表示させ、処理は終了する。

【０１１４】ステップＳ５５において、販売するデジタル情報６が決定されず、中止が要求されたと判定された場合、ステップＳ６３に進み、管理機能２１１は、表示部１２６に処理が中断された旨を示すメッセージを表示させ、処理は終了する。

【０１１５】ステップＳ５７において、デジタル情報鍵および利用条件と共に、ライセンス管理機能付記録媒体１０２－１にデジタル情報６が正常に記録されないと判定された場合、ステップＳ６４に進み、管理機能２１１は、表示部１２６に書き込みが失敗した旨を示すエラーメッセージを表示させ、処理は終了する。

【０１１６】このように、デジタル情報販売装置１０１のデジタル情報６の販売の他の処理によっても、デジタル情報販売装置１０１は、デジタル情報鍵および利用条件と共に、ライセンス管理機能付記録媒体１０２－１にデジタル情報６を記録させることができる。

【０１１７】なお、ステップＳ６１の処理において、料金回収機能２３３が、販売するデジタル情報６の価格に対応する料金を受け取ると説明したが、購入者に、デジタル情報販売装置１０１が設置されている販売店の金銭の支払いをする場所で、ステップＳ５９の処理で印刷された、販売するデジタル情報６の価格を基に、料金を支払わせるようにしてもよい。

【０１１８】上述した一連の処理は、ハードウェアにより実行させることもできるが、ソフトウェアにより実行させることもできる。一連の処理をソフトウェアにより実行させる場合には、そのソフトウェアを構成するプログラムが、専用のハードウェアに組み込まれているコンピュータ、または、各種のプログラムをインストールすることで、各種の機能を実行することが可能な、例えば汎用のパーソナルコンピュータなどに、プログラム格納媒体からインストールされる。

【０１１９】コンピュータにインストールされ、コンピュータによって実行可能な状態とされるプログラムを格納するプログラム格納媒体は、図３に示すように、磁気ディスク１６１（フロッピディスクを含む）、光ディスク１６２（CD-ROM(Compact Disc-Read Only Memory)、ＤＶＤ(Digital Versatile Disc)を含む）、光磁気ディスク１６３（ＭＤ(Mini-Disc)を含む）、若しくは半導体メモリ１６４などよりなるパッケージメディア、または、プログラムが一時的若しくは永続的に格納されるROM１２２や、記録部１２９を構成するハードディスクなどにより構成される。プログラム格納媒体へのプログラムの格納は、必要に応じてルータ、モデムなどの通信部１２８を介して、ローカルエリアネットワーク、インターネット、デジタル衛星放送といった、有線または無線の通信媒体を利用して行われる。

【０１２０】なお、本明細書において、プログラム格納媒体に格納されるプログラムを記述するステップは、記載された順序に沿って時系列的に行われる処理はもちろん、必ずしも時系列的に処理されなくとも、並列的あるいは個別に実行される処理をも含むものである。

【０１２１】また、本明細書において、システムとは、複数の装置により構成される装置全体を表すものである。

【０１２２】

【発明の効果】請求項１に記載の情報販売装置、請求項７に記載の情報販売方法、および請求項８に記載のプログラム格納媒体によれば、販売する情報が蓄積され、情報に対応する利用条件が生成され、情報が暗号化され、暗号化された情報を復号する暗号鍵が生成され、装着されている記録媒体が認証され、認証された記録媒体に、暗号化された情報が利用条件および暗号鍵と共に書き込まれるようにしたので、販売した情報の不正な利用の防止ができるようになる。

【図面の簡単な説明】

【図１】従来のデジタル情報販売システムの構成を説明する図である。

【図２】本発明に係るデジタル情報販売システムの一実施の形態を説明する図である。

【図３】デジタル情報販売装置１０１の構成の例を説明する図である。

＊【図４】本発明に係るデジタル情報販売システムの一実施の形態の構成を説明する図である。

【図５】利用条件およびデデジタル情報鍵が付加されたデジタル情報６を説明する図である。

【図６】デジタル情報販売装置１０１のデジタル情報６の販売の処理を説明するフローチャートである。

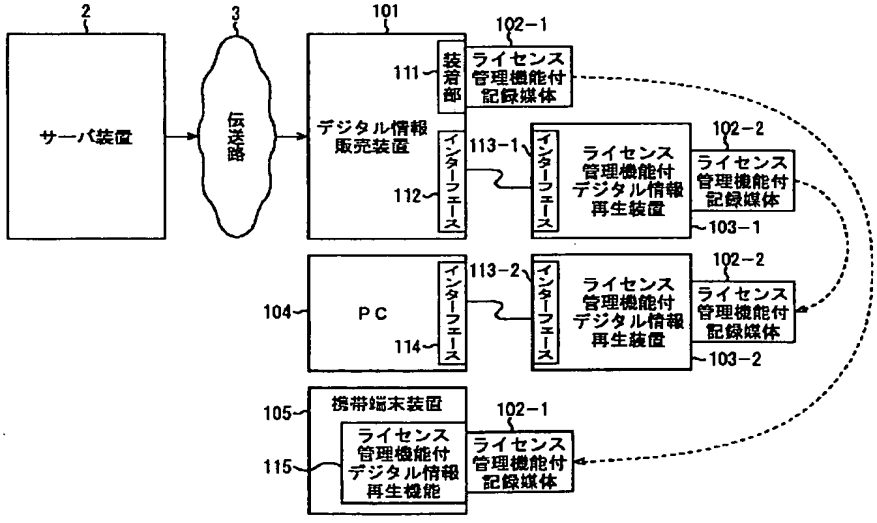
【図７】デジタル情報販売装置１０１の認証機能２１４とライセンス管理機能付記録媒体１０２－１との認証の処理を説明する図である。

【図８】デジタル情報販売装置１０１のデジタル情報６の販売の他の処理を説明するフローチャートである。

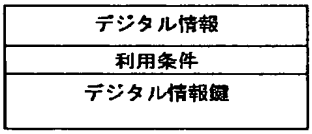
【符号の説明】

１０１　デジタル情報販売装置，　１０２－１，１０２－２　ライセンス管理機能付記録媒体，　１０３－１，１０３－２　ライセンス管理機能付デジタル情報再生装置，　１１２　インターフェース，　１２１　ＣＰＵ，　１２２　ＲＯＭ，　１２３　ＲＡＭ，　１２８　通信部，　１２９　記録部，　１３１　書き込み部，　１３２　料金回収部，　１６１　磁気ディスク，　１６２　光ディスク，　１６３　光磁気ディスク，　１６４　半導体メモリ，　２１１　管理機能，　２１２　デジタル情報蓄積機能，　２１３　デジタル情報販売機能，　２１４　認証機能，　２２７　ライセンス生成機能，　２２８　デジタル情報鍵生成機能，　２２９　暗号化機能，　２３０　ライセンス付デジタル情報書き込み機能

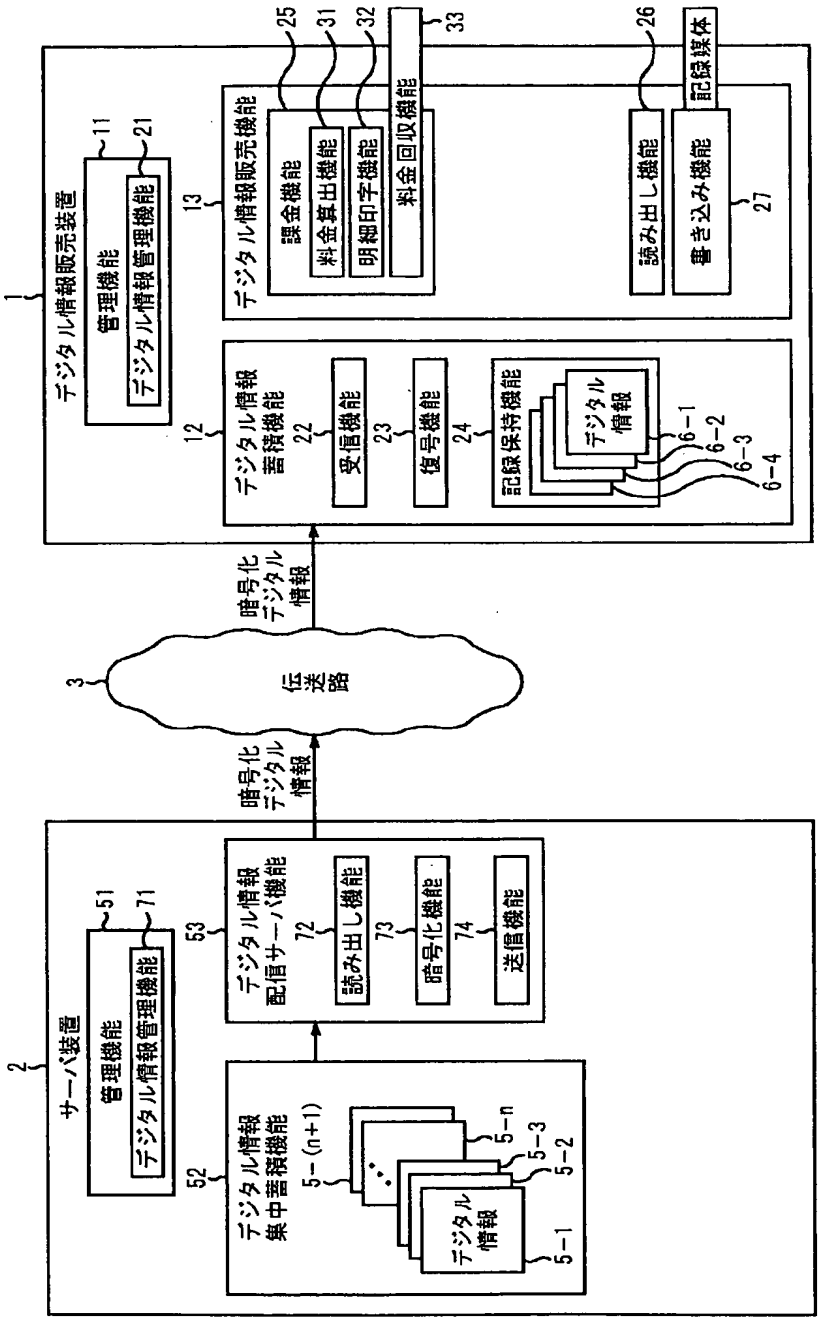
【図２】



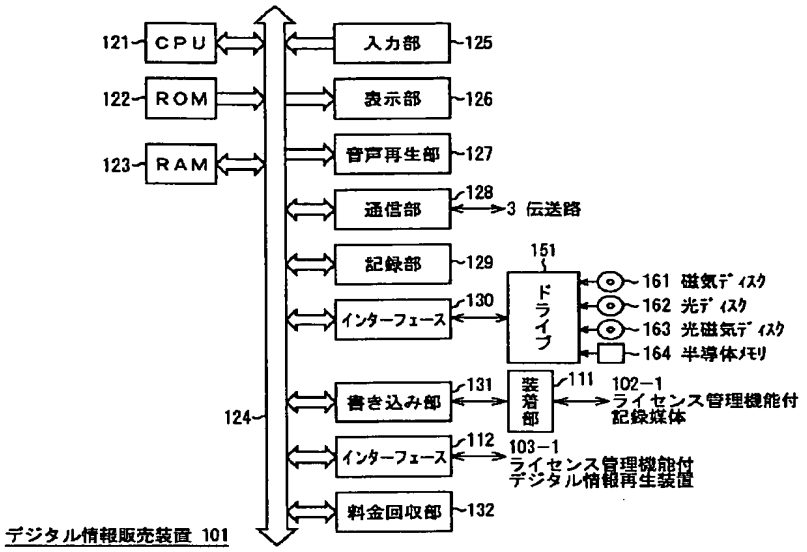
【図５】



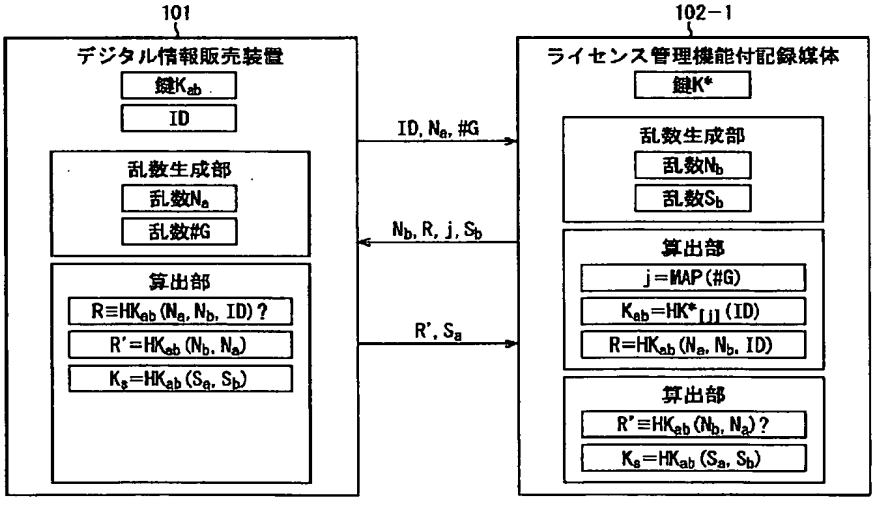
【図１】


サーバ装置
2
管理機能
デジタル情報管理機能
51
71
デジタル情報
集中蓄積機能
52
5-(n+1)
5-n
5-3
5-2
5-1
デジタル情報
配信サーバ機能
53
72
読み出し機能
73
暗号化機能
74
送信機能
暗号化
デジタル
情報
伝送路
3
暗号化
デジタル
情報
デジタル情報販売装置
1
管理機能
デジタル情報管理機能
11
21
デジタル情報
蓄積機能
12
22
受信機能
23
復号機能
24
記録保持機能
デジタル
情報
6-1
6-2
6-3
6-4
デジタル情報販売機能
13
課金機能
料金算出機能
明細印字機能
料金回収機能
25
31
32
33
読み出し機能
書き込み機能
27
26
記録媒体

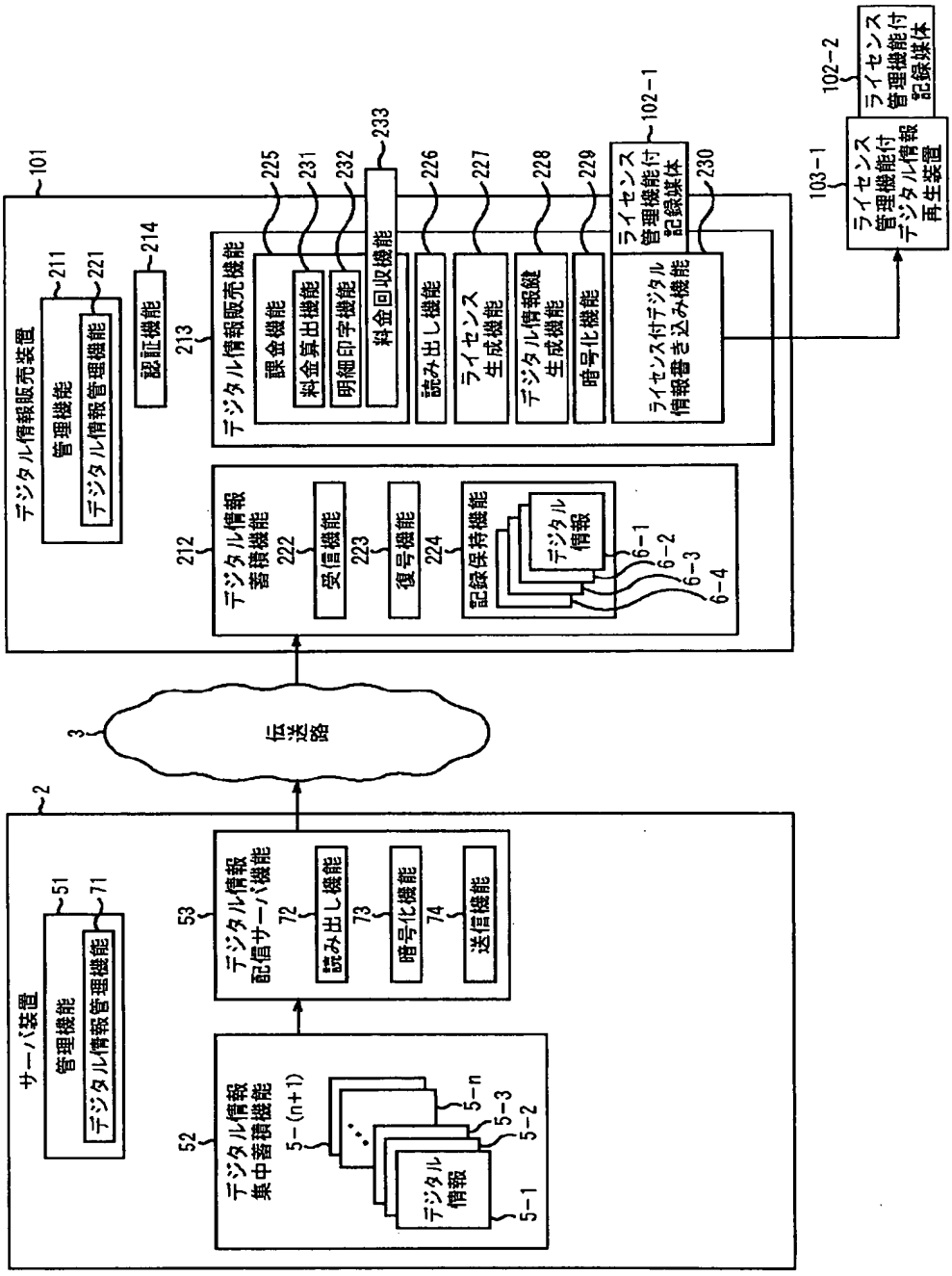
【図３】


121 CPU
122 ROM
123 RAM
124
入力部 125
表示部 126
音声再生部 127
通信部 128
3 伝送路
記録部 129
151
ドライブ
161 磁気ディスク
162 光ディスク
163 光磁気ディスク
164 半導体メモリ
インターフェース 130
書き込み部 131
装着部 111
102−1
ライセンス管理機能付記録媒体
インターフェース 112
103−1
ライセンス管理機能付デジタル情報再生装置
料金回収部 132
デジタル情報販売装置 101

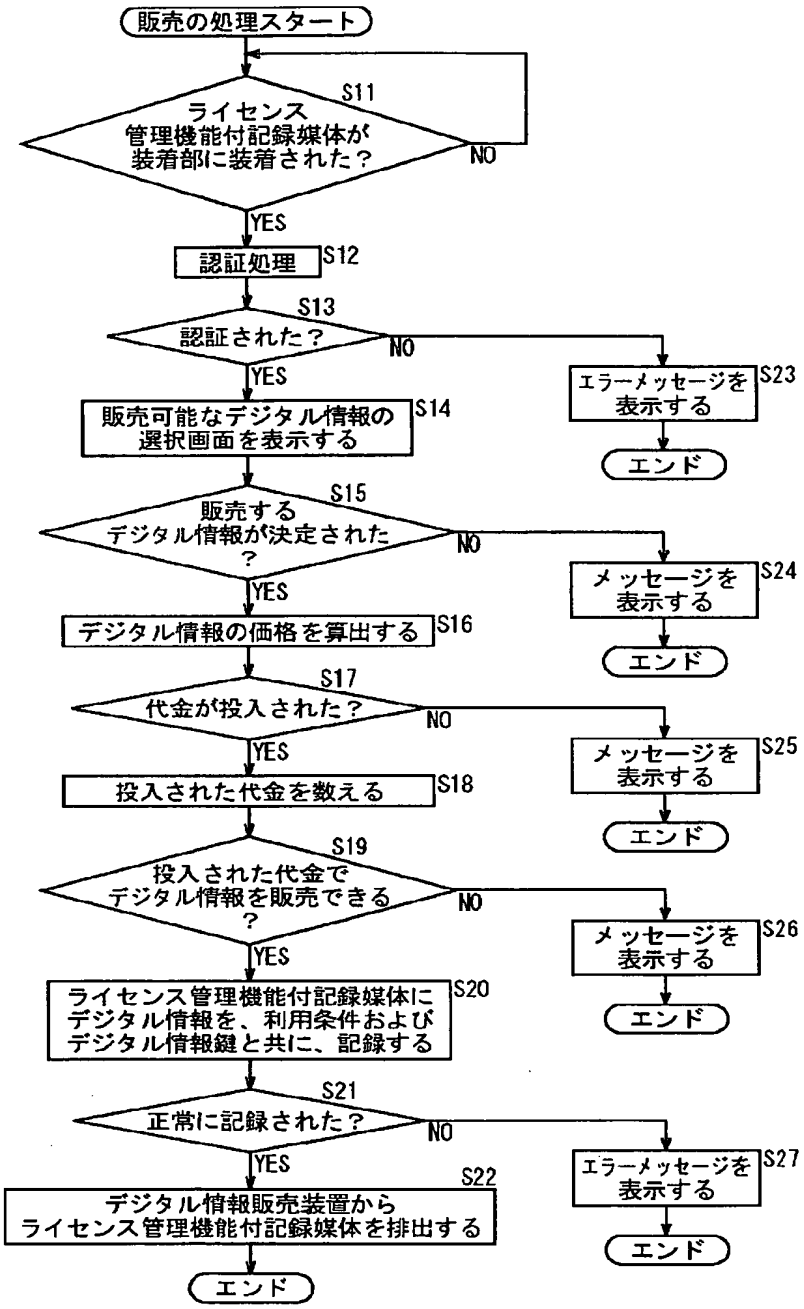
【図７】


101
デジタル情報販売装置
鍵K_{ab}
ID
乱数生成部
乱数N_a
乱数#G
算出部
$R \equiv HK_{ab}(N_a, N_b, ID)$?
$R' = HK_{ab}(N_b, N_a)$
$K_s = HK_{ab}(S_a, S_b)$
ID, N_a, #G
N_b, R, j, S_b
R', S_a
102−1
ライセンス管理機能付記録媒体
鍵K*
乱数生成部
乱数N_b
乱数S_b
算出部
j=MAP(#G)
$K_{ab} = HK^*_{[j]}(ID)$
$R = HK_{ab}(N_a, N_b, ID)$
算出部
$R' \equiv HK_{ab}(N_b, N_a)$?
$K_s = HK_{ab}(S_a, S_b)$

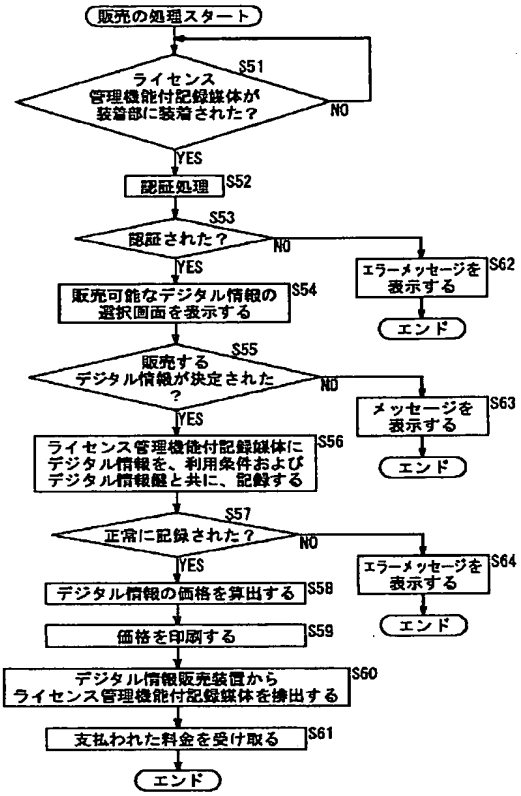
【図４】


101
デジタル情報販売装置
管理機能
211
デジタル情報管理機能
221
認証機能
214
213
デジタル情報販売機能
課金機能
225
料金算出機能
231
明細印字機能
232
料金回収機能
233
読み出し機能
226
ライセンス生成機能
227
デジタル情報鍵生成機能
228
暗号化機能
229
ライセンス管理機能付記録媒体
102-1
230
ライセンス付デジタル情報書き込み機能
デジタル情報蓄積機能
212
受信機能
222
223
復号機能
224
記録保持機能
デジタル情報
6-1
6-2
6-3
6-4
102-2
ライセンス管理機能付記録媒体
103-1
ライセンス管理機能付デジタル情報再生装置
伝送路
3
2
サーバ装置
管理機能
51
デジタル情報管理機能
71
デジタル情報配信サーバ機能
53
読み出し機能
72
73
暗号化機能
74
送信機能
デジタル情報集中蓄積機能
52
5-(n+1)
5-n
5-3
5-2
デジタル情報
5-1

【図６】


販売の処理スタート
S11
ライセンス管理機能付記録媒体が装着部に装着された？
NO
YES
認証処理
S12
S13
認証された？
NO
YES
エラーメッセージを表示する
S23
エンド
販売可能なデジタル情報の選択画面を表示する
S14
S15
販売するデジタル情報が決定された？
NO
YES
メッセージを表示する
S24
エンド
デジタル情報の価格を算出する
S16
S17
代金が投入された？
NO
YES
メッセージを表示する
S25
エンド
投入された代金を数える
S18
S19
投入された代金でデジタル情報を販売できる？
NO
YES
メッセージを表示する
S26
エンド
ライセンス管理機能付記録媒体にデジタル情報を、利用条件およびデジタル情報鍵と共に、記録する
S20
S21
正常に記録された？
NO
YES
エラーメッセージを表示する
S27
エンド
S22
デジタル情報販売装置からライセンス管理機能付記録媒体を排出する
エンド

【図８】



フロントページの続き

(51)Int.Cl.[7]	識別記号	FI		テーマコード(参考)
H04L 9/32		H04N 7/16	Z	
H04N 7/16		H04L 9/00	673B	

Fターム(参考)　5B049 BB00 GG02 GG10
5C064 BA01 BA07 BB05 BB10 BC10
BC17 BC22 BC25 BD02 BD07
BD14
5D044 AB02 AB05 AB07 BC01 BC04
CC04 DE50 EF05 FG18 GK17
HL02 HL04 HL08
5J104 AA01 AA07 AA16 EA04 EA16
KA02 KA06 NA02 PA10 PA14